BEZBEDNOST I ZAŠTITA TELEKOMUNIKACIONIH ŠIROKOPOJASNIH ATM MREŽA

Jeftović V. *Milojko*, Jugoslovenska inženjerska akademija, Beograd,
Pavlović Z. *Boban*, Vojna akademija – Katedra vojnih elektronskih sistema, Beograd

UDC: 621.39
004.724.4

Sažetak:

U radu je prikazana analiza problema bezbednosti i zaštite telekomunikacionih širokopojasnih ATM mreža. Analizirane su brojne moguće pretnje i oblici ugrožavanja širokopojasnih mreža i navedeni zahtevi za bezbednost i zaštitu mreža. Obrađena je koncepcija bezbednosnih mehanizama. Analizirane su bezbednosne mrežne usluge i opisan bezbednosni model ATM mreža. Navedeni su problemi koji se javljaju pri realizaciji bezbednosnih mera i zaštite u komunikaciji preko ATM mreža.

Ključne reči: *asinhroni način transfera – ATM, širokopojasne mreže, bezbednost mreže, pretnje i napadi, zaštita informacija i mreža, bezbednosni sistem, bezbednosne usluge ATM, bezbednosni model ATM mreže, metode zaštite.*

Uvod

Telekomunikacione širokopojasne mreže, poznate kao ATM (engl. *Asynchronous Transfer Mode*) mreže, zasnovane su na principu asinhronog načina transfera (paketski prenos, multipleksiranje i komutacija digitalnih signala) [1]. Definisala ih je i standardizovala Međunarodna unija za telekomunikacije – ITU (engl. *International Telecommunicatios Union*), a uvedene su kao tehnologija za implementaciju širokopojasnih digitalnih mreža integrisanih službi, poznatih kao B-ISDN (engl. *Broadband Integrated Service Digital Networks*). Služe, takođe, i za povezivanje različitih tipova računarskih mreža, povezivanje univerzalnih mobilnih telekomunikacionih sistema i drugih tipova širokopojasnih mreža [4]. Prema mestu u hijerarhijskoj strukturi telekomunikacionog sistema ATM mreže mogu biti kičmene (*backbone*), regionalne ili pristupne, a u zavisnosti od korisnika mrežnih usluga mogu biti privatne ili javne. Ove mreže obez-

vladmijev@ptt.rs

beđuju veoma brojne komunikacione usluge sa zahtevanim ili garantovanim kvalitetom usluga, skraćeno QoS (QoS – *Quality of Service*) [5].

Bez obzira na mesto ATM mreže u strukturi telekomunikacionog sistema, zajednički problem za sve tipove ovih mreža predstavlja njihova bezbednost i zaštita informacija. Polazno pitanje u razmatranju problema bezbednosti i zaštite svakako je analiza pretnji i napada, kojima ATM mreže mogu biti izložene.

Analiza pretnji i napada na telekomunikacione ATM mreže

Problemi bezbednosti i zaštite širokopojasnih mreža mogu se uspešno rešavati samo ako su unapred poznate ili realno procenjene pretnje i napadi kojima mreže mogu biti ugrožene. Studija napada i pretnji potrebna je radi pronalaženja efikasnih mera i tehničkih rešenja za zaštitu.

U poređenju sa mrežama zasnovanim na TCP/IP (*Transmission Control Protocol/Internet Protocol*) protokolima, ATM mreže su mnogo manje bezbednosno ugrožene. Razlog je u tome što se ATM mreže najčešće primenjuju u kičmenoj ravni telekomunikacionog sistema, a kao prenosni medijum koriste optičke kablove. Pored toga, troškovi prisluškivanja ovih mreža mnogo su veći nego što su to troškovi prisluškivanja TCP/IP mreža. Međutim, i ATM mreže su ozbiljno ugrožene nizom različitih vrsta pretnji i napada. Najčešće korišćene pretnje i napadi na ATM mreže su:

1. **Punktiranje optičkog kabla.** Savijanje optičkog vlakna za veoma mali iznos uzrokuje propuštanje svetlosnog signala na mestu savijanja. Do optičkog vlakna u kablu dolazi se relativno lako. Korišćenjem hemijskih rastvarača topi se izolacija, tj. omotač oko optičkog vlakna. Na ogoljeno vlakno preko sonde priključuje se uređaj, koji omogućava da se pristupi svim informacijama, koje se prenose optičkim signalom preko vlakna. Ovakav vid prisluškivanja ne može se detektovati ni na jednom kraju optičkog kabla.

2. **Napad na SDH (Sinhroni Digitalni Hijerarhijski sistem) ili SONET multiplekser (SONET *Drop/Add Multiplex Attacs*).** Meta napada su često SONET optički multiplekseri, koji se uobičajeno štite fizičkim metodama zaštite ormana ili kutija u koje su ugrađeni. Ako fizička zaštita nije efikasna korisničkim podacima se može lako i brzo pristupiti.

3. **Prisluškivanje** je najčešći tip napada na širokopojasnu mrežu, a odnosi se na slučaj kada se napadač direktno priključuje na prenosni medijum ili ga prisluškuje. S obzirom na to da su širokopojasne ATM mreže u najvećem broju slučajeva povezane optičkim kablovima, mogao bi se steći pogrešan utisak da se one ne mogu prisluškivati. Oprema za prisluškivanje optičkog vlakna je relativno jeftina (oko 2000 dolara). Napadač treba dobro da poznaje strukturu multipleksnog rama SDH (sinhronih digitalnih hijerar-

hijskih) ili SONET sistema, kao i komunikacione protokole kojima se obavlja komunikacija porukama (govor, podaci, video slika, grafika, mirna slika, multimedijalne poruke i dr.), a takođe i arhitekturu ATM komunikacionih protokola. Problem je kako otkriti da li se optička transmisiona mreža prisluškuje. Interesantno rešenje je primenjeno u zgradi američkog Ministarstva odbrane, tj. u Pentagonu. Računarska mreža Pentagona realizovana je ugradnjom, odnosno korišćenjem optičkih kablova. Optički kablovi provučeni su kroz cevi sa gasom pod povišenim pritiskom. U kontrolnim tačkama neprestano se prati vrednost pritiska u gasnim cevima, a minimalna promena pritiska ukazuje na pokušaj prisluškivanja mreže.

4. **Prevara** je oblik napada na ATM mrežu kada se napadač pretvara da je neko drugi, da bi dobio dozvolu za pristup podacima za koje nema odobrenje ili da bi naneo štetu nekom legalnom korisniku mrežnih usluga. Ovaj oblik napada zasniva se na nekim karakteristikama ATM komutacionih sistema. Većina ATM komutacionih sistema ima specijalne portove, namenjene za korišćenje u slučaju da se pojave problemi u obezbeđenju zahtevanih veza i pristupu svim podacima, video i audio signalima. Pristup svim signalima, koji prolaze kroz komutacioni sistem, ostvaruje se korišćenjem jednostavnog programa za „skidanje“ šifre na portovima komutacionog sistema. Ovakva vrsta napada ponekad zahteva posebne softverske alate za manipulisanje jedinicama podataka protokola (PDU – *Protocol Data Unit*), odnosno sadržaju informacionog polja ATM protokola. Obično sa kao mera zaštite od neovlašćenog korisnika u pristupu portovima zahteva posebno odobrenje koje napadač mora da ima, na primer, da je registrovan kao *super user* u UNIX okruženju. S obzirom na to da su ATM mreže povezane sa mnogim nezaštićenim javnim mrežama, napadača je nemoguće sprečiti da dođe do ovakvog odobrenja za pristup. S obzirom na to da se širokopojasne ATM mreže koriste u u okruženju javnih mreža, one će uvek biti meta prethodno navedene vrste napada.

5. **Krađa virtuelnog kanala.** Ova vrsta napada odnosi se na mogućnost da napadač neovlašćeno koristi virtuelni kanal (VC – *Virtual Channel*) od drugog korisnika. Na primer, neka su VC1 i VC2 dva virtuelna kanala od ATM komutatora A do ATM komutatora B, a koji pripadaju različitim korisnicima U1 i U2. Ako komutatori A i B imaju kompromis, onda komutator A može komutirati ćelije virtuelnog kanala VC1, od A ka B, preko virtuelnog kanala VC2, a zatim te ćelije komutator B vraća nazad po virtuelnom kanalu VC1. S obzirom na to da ATM komutatori prosleđuju ćelije na osnovu identifikatora virtuelnog kanala VCI (engl. *Virtual Channel Identifier*) i identifikatora virtuelnog puta VPI (engl. *Virtual Path Identifier*) koji se nalaze u zaglavlju svake ćelije, komutatori A i B mogu samo zamenjivati ova polja i ponovo vratiti ćelije. Komutatori A i B neće primetiti ove promene i komutiraće ćelije virtuelnog kanala VC2, kao da su to originalne ćelije tog kanala. U ATM mreži u kojoj je garantovan kvalitet usluga, korisnik U1 može puno dobiti ako neovlašćeno koristi kanal korisnika U2, koji je, na primer, mnogo boljeg kvaliteta za koji U1 nije ovlašćen.

6. **Odbijanje usluga.** Usluge se odbijaju kada neki entitet u mreži ne može da izvrši svoju funkciju ili kada sprečava druge entitete da izvrše funkcije. Pod odbijanjem usluga smatra se i sprečavanje pristupa ATM uslugama ili sprečavanje komutacije ako se, na primer, ATM mreža preplavi nepotrebnim saobraćajem.

Treba imati u vidu da se u ATM mreži komunikacija ostvaruje po uspostavljenoj vezi preko virtuelnih kanala i virtuelnih puteva. Vezom, odnosno uspostavom virtuelnog kola, upravlja se skupom signala. Tako se virtuelni kanal uspostavlja SETUP signalom, a veza se može raskinuti signalima RELEASE ili DROP PARTY. Ako napadač često šalje RELEASE ili DROP PARTY signale, on može znatno da naruši komunikaciju između korisnika i na taj način degradira kvalitet usluga u ATM komunikaciji. Pomenuta vrsta napada može se manifestovati i kao generisanje ekstra-saobraćaja, koji preplavljuje mrežu, a istovremeno sprečava druge korisnike da koriste mrežne usluge ili odlaže njihov saobraćaj.

7. **Slabosti ATM protokola**. ATM protokoli ne podležu autentifikaciji sadržaja niti su ćelije šifrovane. Posledica ove činjenice jeste rizik od moguće prevare. Ako se napadač na mrežu pretvara da je poverljivi komutator, moguće je ostvariti pristup jednom portu u ATM komutatoru i kontrolisati rutiranje poruka ili podataka kroz komutaciono polje. To se može izvesti bez bilo kakvog pristupa mrežnom interfejsu upravljačkog modula ATM komutatora.

8. **Analiza saobraćaja**. Ova pretnja odnosi se na slučaj kada napadač može dobiti važne informacije sakupljanjem i analizom podataka kao što su volumen, vremensko trajanje (tajming) zauzeća, kao i drugih komunikacionih elemenata određenog virtuelnog kanala. Volumen i tajming mogu otkriti mnoge važne informacije, čak i u slučaju kada su poruke koje se prenose šifrovane, zato što kriptozaštita nema efekta na volumen i tajming poruka.

9. **ILMI napadi.** ILMI (engl. *Integrated Local Management Interface*) protokol koristi se na interfejsu između privatne i javne ATM mreže, odnosno između radne stanice (terminal) i ATM komutatora. Protokol ILMI je baziran na SNMP (engl. *Simple Network Management Protocol*) protokolu. ILMI ne obezbeđuje mehanizme za autentifikaciju, pa napadač, koji se ne mora autentifikovati, može iskoristiti ILMI da bi registrovao dodatne ATM adrese za svoju radnu stanicu. Korišćenjem dodatno registrovanih adresa napadač može premostiti adresne filtre koji su konfigurisani na ATM komutatoru. Napadač, takođe, sa protokolom ILMI može pokušati da se registruje preko neke ranije isključene radne stanice. ILMI se, takođe, može koristiti za automatsko konfigurisanje tipa interfejsa ATM komutatora. Napadač može koristiti ILMI da bi se predstavio kao ATM komutator, postavljanjem tipa interfejsa na NNI (engl. *Network to Network Interface*). Pri tome se nepouzdani UNI (engl. *User Network Interface*) port konfiguriše u pouzdani NNI port pomoću napadačeve ILMI poruke. Nakon toga moguće je napasti rutiranje javne ATM mreže preko PNNI interfejsa (engl*. Private Network to Network Interface*).

10. **PNNI napadi**. PNNI je hijerarhijska šema rutiranja unutar javnog ATM komutatora. Korišćenjem PNNI HELLO signalizacionih poruka mrežni elementi razmenjuju informacije o stanju linkova da bi izabrali tzv. lidera „peer“ grupe (engl. *Peer Group Leader* – PGL). PGL se tada označava kao komutator, a zadužen je za interakciju sa elementima izvan lokalne „peer“ grupe. Ove signalizacione poruke šalju se u jasnoj formi bez autentifikacije. Napadaču je dovoljno da sastavi HELLO signalizacionu poruku sa lažnim ATM adresama, tako da može označiti komutator pod svojom kontrolom kao PGL. Kada jednom stekne kontrolu nad PGL, napadač dobija kontrolu nad rutiranjem poruka (podaci, govor, video slika, itd.) u ATM komutatoru, pa jednostavno može „hvatati“ željene poruke ili blokirati komunikaciju cele „peer“ grupe, odnosno izazvati propadanje cele ATM mreže. Napadač, takođe, može iskoristiti i odgovor na HELLO poruku PGL i ubaciti zlonamerne informacije o stanju linkova, koje će PGL pridružiti svim članovima grupe. Članovi PGL će na osnovu toga doneti pogrešna pravila rutiranja poruka u ATM mreži.

Zahtevi za bezbednost mreže i zaštitu informacija

Da bi se osigurala bezbednost i zaštita ATM mreža definisani su precizni tehnički zahtevi, koji se moraju zadovoljiti. Najvažnija četiri osnovna zahteva za bezbednost ATM mreža su:

– autentifikacija (engl. *Authentication*) – utvrđivanje identiteta učesnika u komunikaciji,

– tajnost (engl. Confidentiality) – isključivo ovlašćeni učesnici mogu pristupiti sadržaju poruka,

– integritet (engl. *Integrity*) – u toku prenosa ne sme doći do promene sadržaja poruke,

– neporicanje (engl. *Non-repudiation*) – korisnik, učesnik u komunikaciji, ne sme poreći činjenicu da je pristupio mrežnim uslugama ili porukama.

Pod autentifikacijom se podrazumeva utvrđivanje identiteta sagovornika pre početka prenosa poruka kroz mrežu. Ona omogućava verifikaciju da su učesnici u komunikaciji zaista oni za koje se predstavljaju. U javnim, kao i u privatnim mrežama, zahteva se da sve bude autentifikovano, uključujući i šifarske ključeve.

Tajnost informacija obezbeđuje se šifrovanjem, tajnim ili javnim ključem. Time se obezbeđuje zaštita od neautorizovanog pristupa. Tajnošću ostvarenom šifrovanjem, takođe se obezbeđuje zaštita i korektnost distribucije simetričnog ključa.

Integritet poruka se proverava na strani koja prima poruku. Prijemna strana ima mogućnost verifikacije da je primljena poruka stigla bez ikakvih izmena.

Sistemi za šifrovanje, pored zaštite tajnosti sadržaja poruka, takođe služe za autentifikaciju i proveru integriteta poruka. Pored pomenutih zahteva, bezbednosni sistem ATM mreža treba da obezbedi usluge sigurnog upravljanja šifarskim ključevima i distribuciju ključeva, kao i kontrolu pristupa korisnika ATM mreži.

Kontrola pristupa korisnika širokopojasnoj mreži ATM značajnija je nego u drugim vrstama mreža. Treba imati u vidu da ATM mreže garantuju kvalitet usluga (QoS) u komunikaciji. QoS se obezbeđuje klasifikacijom saobraćaja u različite klase i usmerava različitim prioritetom i kvalitetom kanala. Ako bi pristup korisnika mreži bio neograničen onda garancija kvaliteta ne bi imala smisla.

Osnovu bezbednosnog sistema čine algoritmi upravljanja ključevima. S obzirom na to da se bezbednost informacija ostvaruje postupkom šifrovanja/dešifrovanje, pa ako napadač dođe do ključa, koji se koristi u pomenutom procesu, kompletan bezbednosni sistem biće razbijen. U velikim telekomunikacionim ATM mrežama, zbog velikog broja učesnika u distribuciji ključeva, upravljanje se ne može vršiti manuelno, već automatski ili poluautomatski. Zbog toga je izuzetno težak problem kako osigurati ključeve prilikom njihovog prenosa kroz mrežu.

Bezbednosni ciljevi i funkcije bezbednosnog sistema ATM mreža

Radna grupa ATM Foruma za pitanja bezbednosti, u februaru 1997. godine, predložila je nacrt bezbednosnog okvira za ATM, koji je odobren od strane tehničkog odbora ATM Foruma (engl. *ATM Forum Technical Committee*) pod nazivom *ATM Security Framework 1.0*. Ovim dokumentom precizno su definisani bezbednosni ciljevi i tehnički zahtevi za bezbednost i zaštitu ATM mreža [1].

Definisanju zahteva prethodila je analiza bezbednosnih ciljeva, a pre svega ciljeva određenih interesnih grupa:

– korisnika, odnosno korisnika i pretplatnika usluga,

– operatora (mrežni operatori i provajderi, odnosno davaoci usluga),

– javnog sektora.

Korisnički ciljevi nisu uniformni zbog toga što svaki korisnik ima svoje ciljeve. Oni se mogu svesti na:

– raspoloživost i ispravno funkcionisanje usluge, njeno pouzdano aktiviranje i deaktiviranje,

– korektnu naplatu i mogućnost provere računa,

– obezbeđenje tajnosti poruka, odnosno informacija,

– mogućnost anonimnog korišćenja usluga.

Cilj mrežnih operatora i provajdera usluga jeste da ostvare što veći prihod i zaradu od korisnika usluga ATM mreže. Ovaj cilj uključuje maksimalan prihod ostvaren od mrežnih usluga i minimalne troškove nastale zbog neovlašćenog korišćenja mrežnih usluga. Cilj operatora i provajdera usluga ostvaruje se kroz:

– raspoloživost i ispravnost funkcionisanja ATM mrežnih usluga,

– raspoloživost i ispravno funkcionisanje ATM mrežnog menadžmenta,

– ispravnu naplatu i mogućnost provere računa, pre svega bez mogućnosti prevare,

– očuvanje sopstvene reputacije (pre svega očuvanje korisničkog i investitorskog poverenja),

– odgovornost za sve aktivnosti u ATM mreži, i

– integritet podataka i tajnost poruka u prenosu kroz mrežu.

Cilj javnog komunukacionog sistema je garancija:

– raspoloživosti i ispravnosti funkcionisanja ATM mrežnih usluga, i

– tajnosti poruka u prenosu preko mreže.

Na osnovu prethodno pomenutih ciljeva definisani su glavni ciljevi za bezbednost ATM mreža, a to su: tajnost (engl. *Confidentiality*), integritet poruka/informacija (engl. *Data Integrity*), odgovornost (engl. *Accountability*) i raspoloživost (engl. *Availability*). Tajnost i integritet informacije obezbeđuje se s kraja na kraj veze upotrebom korisničkih terminala koji podržavaju pomenute funkcije [2]. Pod odgovornošću se podrazumeva obezbeđenje mrežnih funkcija autentifikacije i neporicanja, kao i odgovornost entiteta za sve aktivnosti koje su inicirali u mreži.

Koncepcija i primena bezbednosnih usluga

U skladu sa prethodno navedenim ciljevima definisane su funkcije koje treba da ima bezbednosni sistem ATM mreže [7]. To su:

– verifikacija identiteta. Bezbednosni sistem treba da utvrdi i verifikuje identitet bilo kojeg učesnika u ATM mreži;

– kontrolisani pristup i ovlašćenje (engl. *Authorization*). Kontrolom pristupa i ovlašćenja sprečava se pristup informacijama i resursima za koje nisu ovlašćeni;

– zaštita tajnosti. Podaci koji se prenose preko mreže, kao i podaci memorisani unutar mreže moraju biti zaštićeni;

– zaštita integriteta podataka. Bezbednosni sistem treba da garantuje integritet memorisanih podataka, kao i podataka koji se prenose u komunikaciji kroz mrežu;

– stroga odgovornost. Entiteti u mreži ne mogu poreći odgovornost za akcije koje preduzimaju, kao ni za njihove efekte;

– aktivnosti logovanja (engl. *Activities Loging*). Bezbednosni sistem treba da podrži mogućnost pronalaženja informacija o bezbednosnim aktivnostima u mrežnim elementima uz mogućnost povezivanja ovih informacija sa pojedinim korisnicima ili entitetima;

– prijava alarma. Bezbednosni sistem treba da ima mogućnost generisanja alarma u slučaju pojave određenih događaja, vezanih za bezbednost;

– provera. Kada se desi prekršaj bezbednosnih mera, odnosno ako se naruši bezbednost, sistem treba da omogući analizu svih ulaznih podataka, unetih logovanjem, koji su bitni za bezbednost;

– bezbednosni oporavak (engl. *Security Recovery*). Sistem treba da ima mogućnost oporavka u slučaju prekršaja mere bezbednosti ili pokušaja narušavanja bezbednosti;

– bezbednosno upravljanje (engl. *Security Management*). Bezbednosni sistem treba da ima mogućnost upravljanja bezbednosnim uslugama izvedenim prema prethodno navedenim zahtevima.

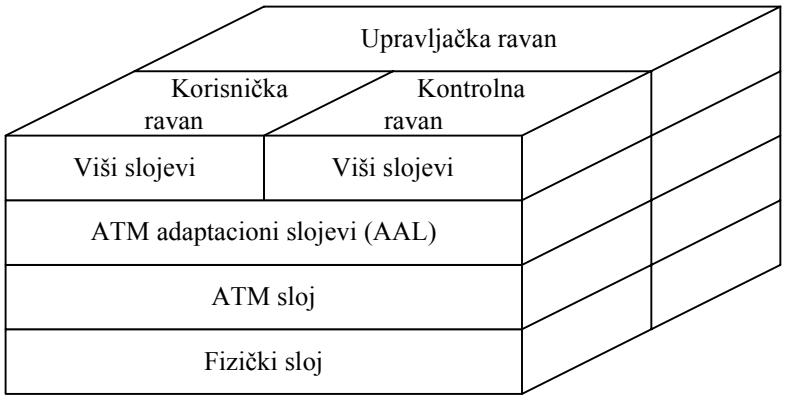
Poslednja dva zahteva ne obezbeđuju bezbednosne usluge već predstavljaju osnovu bezbednosnog sistema. Neophodni su za održavanje bezbednosnih usluga.

Treba imati u vidu da su različiti primeri ATM mreža izloženi različitim vrstama napada, pa zbog toga različite ATM mreže imaju različite bezbednosne ciljeve. U zatvorenom mrežnom okruženju dovoljan nivo bezbednosti može se ostvariti načinom organizacije, a zasniva se na relativno poverenju unutar organizacije ili između grupa organizacija, koje koriste ATM mrežu. Za posebne korisnike ATM mreža vrši se procena rizika izradom tzv. studije pretnji, kojom se definiše koji bezbednosni zahtevi moraju biti ponuđeni i ispunjeni.

Primena bezbednosnih usluga

Nakon analize mogućih pretnji i napada na ATM mrežu i definisanja bezbednosnih zahteva, treba odrediti bezbednosne usluge, kao i način primene ovih usluga na ATM mrežnu arhitekturu. Da bi se rešio problem bezbednosti ATM mreža, a takođe definisala ATM bezbednosna infrastruktura, tehnički komitet (*Tecnical Committee*) ATM Foruma, u februaru 1999. godine, usvojio je bezbednosnu specifikaciju pod nazivom *ATM Security Specification Version 1.0*, koja predstavlja napor da se definišu procedure uvođenja bezbednosnih usluga u ATM mreže.

ATM bezbednosna specifikacija, predstavljena referentnim modelom arhitekture ATM protokola, prikazana je na slici 1.



Slika 1 – Arhitektura ATM protokola

Model arhitekture ATM protokola, simbolično predstavljen kockom, čine tri ravni: korisnička ravan, kontrolna ravan i upravljačka ravan. Ovakav način predstavljanja je pogodan radi lakšeg uočavanja složenih komunikacionih funkcija koje se obavljaju u ATM mreži.

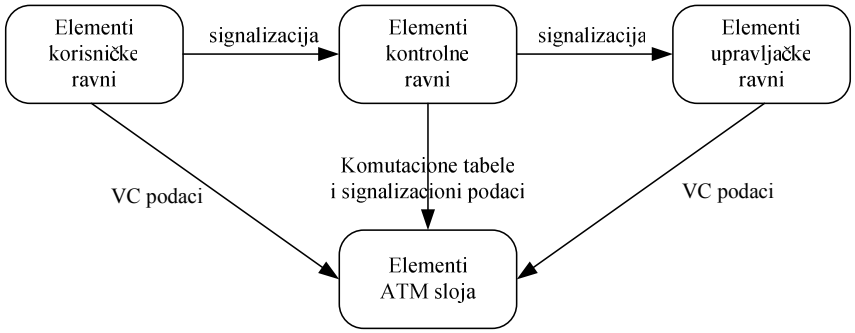
Korisnička ravan. Protokoli ove ravni podržavaju prenos i komutaciju korisničkih informacija, uspostavu, održavanje i raskidanje veza, zajedno sa protokolima kontrolne ravni. Prenos korisničkih poruka kroz komutiranu ATM mrežu ostvaruje se komutacijom virtuelnih kola (VC) i virtuelnih puteva (VP).

Kontrolna ravan. Protokoli kontrolne ravni vrše funkcije kontrole poziva i kontrolu veza, odnosno obavljaju uspostavu, održavanje i raskidanje veza, uključujući UNI, NNI i ICI (*Interface Control Information*) signalizaciju na različitim mrežnim interfejsima.

Upravljačka ravan. Upravljačka ravan upravlja prethodno navedenim ravnima i njihovim slojevima, obavlja upravljačke funkcije koje se odnos na celu mrežu i obezbeđuje koordinaciju između sve tri ravni.

Svaka od navedenih ravni sadrži tri sloja protokola: fizički sloj, ATM sloj, ATM adaptacioni sloj (AAL), kao i više slojeva ako se to zahteva u određenim ATM vezama. U prenos poruka (govor, tekst, podaci, video itd.) neposredno su uključena samo prva tri sloja protokola. ATM sloj je zajednički za sve usluge koje omogućavaju paketski prenos. AAL, odnosno protokoli ovog sloja zavisi od usluge koju ATM mreža pruža korisnicima. AAL sloj prima poruke od aplikacije (viših slojeva) i segmentira ih u blokove od po 48 bajtova, koje zatim šalje ATM sloju. Takođe AAL sloj prima poruke – pakete sa po 48 bajtova i prosleđuje ih višim slojevima. ATM sloj na svaki blok dodaje zaglavlje sa 5 bajtova i na taj način formira ćelije fiksne dužine od 53 bajta. Zaglavlje ćelije sadrži zaglavlje sa informacijama potrebnih za komutaciju, transport i usmeravanje do naznačenog odredišta. ATM sloj šalje ATM ćelije fizičkom sloju čije su funkcije i karakteristike određene prenosnim medijumom i načinom kodovanja signala.

Ravni u referentnom modelu ATM protokola sadrže entitete. Entitet je nešto što je sposobno da prima i otprema podatke. Model interakcije između ATM entiteta prikazan je na slici 2.



Slika 2 – Model interakcije između ATM entiteta

Entitet u korisničkoj ravni se koristi za prenos korisničkih poruka. Entiteti u kontrolnoj ravni rade sa konekcionim funkcijama, kao što su uspostava veze, održavanje i raskidanje veza i druge. Entiteti upravljačke ravni vrše upravljanje i koordinaciju funkcija korisničke i kontrolne ravni. Upravljačka ravan uključuje i funkcije za uspostavljanje infrastrukture rutiranja između interfejsa čvorova privatnih ATM mreža. Pored entiteta pomenute tri ravni postoje i entiteti ATM sloja. Entiteti ATM sloja vrše ATM prenos podataka u ime drugih entiteta iz sve tri ravni.

Da bi se bezbednosni zahtevi primenili na celu ATM mrežu jasno je da sve tri ravni i ATM sloj moraju biti predmet zaštite.

U martu 2001. godine, Tehnički komitet ATM Foruma usvojio je novu verziju bezbednosne specifikacije pod nazivom *ATM Security Spesification Version 1.1.* Nova verzija je ispravila neke greške iz prethodne verzije i dopunila neke delove. Obim bezbednosti koji je definisan u specifikaciji ostao je isti. U Tabeli 1 sa X su obeležene oblasti koje su definisane u pomenutoj specifikaciji. Prazna polja u tabeli pokazuju da upravljačka ravan nema nikakvu zaštitu, a da se tajnost i kontrola pristupa ne obezbeđuju u kontrolnoj ravni. Potpuna zaštita se preporučuje za korisničku ravan.

Tabela 1

Oblasti bezbednosti prema ATM specifikaciji verzija 1.1

Bezbednosna oblast / Usluge	Korisnička ravan	Kontrolna ravan	Upravljačka ravan
Autentifikacija	X	X	
Tajnost	X		
Integritet podataka	X	X	
Kontrola pristupa	X		

ATM bezbednosna specifikacija određuje mehanizme za autentifikaciju, tajnost, integritet podataka i kontrolu pristupa za korisničku ravan. Takođe specificira mehanizme za autentifikaciju i integritet za kontrolnu ravan (UNI i NNI signalizacija). Iz područja zaštite, prema specifikaciji isključena je zaštita upravljačke ravni. Međutim, kako entiteti upravljačke ravni koriste veze korisničke ravni da bi izvršili svoje funkcije, onda i specifikacija bezbednosti korisničke ravni može doprineti ostvarenju zaštite upravljačke ravni. Takođe u specifikaciji je određena i infrastruktura potrebna za podršku pomoćnih bezbednosnih usluga: dogovaranje bezbednosnih usluga i parametara, razmena ključeva i sertifikacija infrastrukture.

Oblast koja je obuhvaćena ATM specifikacijom 1.1 ograničena je na mehanizme koji moraju biti primenjeni u ATM sloju i/ili AAL sloju. Ovo je naglašeno kroz ostvarivanje bezbednosti prvenstveno po uspostavljenoj vezi, a ne radi ostvarivanja zaštite po linkovima i čvorovima (ATM komutacioni sistemi). To znači da se štiti uspostavljena veza, a ne link ili mrežni čvor. Predmet zaštite, radi ostvarivanja bezbednosti, obuhvata kanal i putanju poruke, veze tačka – tačka i tačka – više tačaka, kao i komutirane i permanentne veze.

Bezbednosne ATM mrežne usluge

Kao što je prethodno naglašeno, bezbednosna specifikacija, pa time i bezbednosne usluge, odnose se na bezbednosne mehanizme u korisničkoj ravni i delom u upravljačkoj ravni. Otuda potreba da se detaljnije analiziraju bezbednosne usluge korisničke ravni.

Bezbednosne usluge korisničke ravni

Da bi se zadovoljili korisnički bezbednosni ciljevi, korisnička ravan treba da obezbedi korisničke usluge kao što su kontrola pristupa, autentifikacija, tajnost poruka i integritet. Isto tako, bezbednost korisničke ravni treba da bude dovoljno fleksibilna da bi se zadovoljili korisnički zahtevi, s obzirom na to da različite veze imaju različite zahteve u pogledu bezbednosti. Zbog različitih klasa saobraćaja u ATM mreži, važno je ponuditi različite opcije bezbednosnih usluga. Druge usluge, kao što su razmena ključeva, sertifikacija infrastrukture i dogovaranje bezbednosnih opcija, mogu biti korisne zbog raznolikosti korisničkih zahteva. Zbog toga one treba da budu podržane u korisničkoj ravni.

Prema ATM specifikaciji 1.1, bezbednosne usluge krisničke ravni primenljive su na bazi veze ostvarene preko virtuelnog kola VC (*Virtual Circuit*), gde VC može biti veza preko virtuelnog kanala VCC (*Virtual Circuit Connection*) ili veza virtuelnog puta VPC (*Virtual Path Connection*). Bezbednosne usluge za fizički link, koji može prenositi veliki broj VC, nisu predviđene.

Za korisničku ravan su definisane sledeće usluge: autentifikacija, tajnost poruka, integritet poruka i kontrola pristupa. Ove usluge se odnose na veze tačka – tačka i tačka – više tačaka i to za komutirana virtuelna kola (SVC) i permanentna virtuelna kola (PVC). Na krajevima VC ili duž putanje VC postavljaju se tzv. bezbednosni agenti, SA (*Security Agent*). SA je entitet koji inicira, uspostavlja, obezbeđuje, prekida i okončava bilo koju od bezbednosnih usluga. Drugim rečima, bezbednost se realizuje između bezbednosnih agenata.

Kontrola pristupa u zaštiti korisničke ravni se koristi da bi se učesnicima koji nisu ovlašćeni, sprečilo uspostavljanje veze. Da bi specifikacija bila nezavisna od implementacije, standardizovane su informacije i mehanizam rezmene informacija koje zahteva posebni algoritam za kontrolu pristupa.

Autentifikacija. Autentifikacija se koristi da bi se utvrdilo da li su pozivajuća i pozvana strana zaista one za koje se predstavljaju. Autentifikacija je prvi korak u komunikaciji koja se, prema Specifikaciji 1.1, obavlja pomoću tehnike kriptozaštite algoritmima sa simetričnim i asimetričnim ključem. Mehanizam obezbeđenja tajnosti realizuje se na nivou svake ćelije. Drugim rečima, šifruje se korisnički sadržaj svake ćelije, tako da on nije dostupan neovlašćenom korisniku. Zaglavlje ćelije se ne šifruje, niti se u zaglavlje unose bilo kakve izmene.

Prema pomenutoj specifikaciji integritet podataka kao usluga je odvojen od tajnosti podataka. Ovo razdvajanje omogućava da usluge integriteta podataka budu primenjene na nivou AAL jedinice podataka usluge SDU (*Service Data Unit*). To znači da se za AAL-SDU jedinicu određuje digitalni potpis i on se dodaje AAL-SDU jedinici. Primalac poruke može na ovaj način da utvrdi da li su podaci u svakoj ćeliji menjani ili nisu.

Autentifikacijom korisničke ravni, na početku komunikacije određuje se da li su identiteti pozivajuće i/ili pozvane strane verodostojni. Kako ova usluga obezbeđuje zaštitu od lažnog predstavljanja ili napada prevarom, ona je od esencijalne važnosti za sigurnu komunikaciju. Iz tog razloga, autentifikacija je neophodna za rad drugih bezbednosnih usluga, uključujući razmenu ključa, kao i sigurnu razmenu dogovorenih bezbednosnih parametara.

Autentifikacija može biti obostrana (engl. *mutual*) ili jednostrana (engl. *unilateral*). Kod obostrane, vrši se istovremena identifikacija obe strane, a kod jednostrane, samo jedna strane se autentifikuje drugoj strani.

Prema Specifikaciji 1.1, autentifikacija se vrši pomoću kriptografskih algoritama uz korišćenje algoritama sa asimetričnim (javnim) ključem (na primer RSA – algoritam koji su predložili Rivest R., Shamir A. i Adleman L. i koji je dobio naziv prema početnim slovima prezimena svakog od tri autora) i algoritme sa simetričnim (tajnim) ključem, kao što je, na primer, DES-MAC (*Data Encryption Standard – Message Authentication Code*).

Tajnost. Ovom uslugom korisničke ravni obezbeđuju se kriptografski mehanizmi koji štite korisničke poruke od neovlašćenog otkrivanja. U ovom slučaju pojam korisnik se odnosi na entitet protokola koji direktno koristi ATM usluge. Specifikacijom verzije 1.1, definiše se tajnost na nivou ćelije (ATM sloj). Ovo je bolje rešenje nego da se šifrovanje obavlja na AAL sloju, jer se sa fiksnom dužinom ćelije ostvaruje efikasnije šifrovanje. Kako je prethodno pomenuto, šifruje se samo korisnički sadržaj, a zaglavlje ćelije ostaje otvoreno. Na ovaj način se omogućava velika brzina komutacije bez potrebe za dešifrovanjem/šifrovanjem u komutacionom polju ATM komutatora. Za usluge tajnosti u pomenutoj specifikaciji je određeno da se koriste simetrični algoritmi (sa tajnim ključem) za šifrovanje (na primer DES, *Triple*-DES). Simetrični algoritmi su mnogo brži što ih čini mnogo upotrebljivijim za šifrovanje ATM ćelija, odnosno poruka.

Integritet. Usluge integriteta poruka obezbeđuju mehanizmi za detekciju promena sadržaja poruka ili sadržaja sekvenci, odnosno delova neke poruke, posebno u prisustvu zlonamernih mogućnosti promena. Ova usluga je predviđena za korišćenje između krajnjih tačaka (s kraja na kraj veze) na AAL-SDU nivou, a za protokole AAL 3/4 i AAL 5. Kao dodatak, ponuđene su dve opcije za ovu uslugu, prva – integritet poruka bez *replay/reordering* zaštite, i druga, sa *replay/reordering* zaštitom.

Kada se integritet primenjuje bez *replay/reordering* zaštite, izvor pre otpreme dodaje kod za autentifikaciju poruke MAC (*Message Authentication Code*) na kraj (rep) svake AAL-SDU jedinice. Vrednost MAC se računa nad celom AAL-SDU. Ova opcija je korisna za protokole viših slojeva, koji imaju svoj lični broj sekvence (npr. protokol TCP), jer bi dupliranje ove funkcija na AAL nivou bilo nepotrebno. Kada su ponuđene odnosno primenjene usluge integriteta poruka sa *replay/reordering* zaštitnom funkcijom, usluge integriteta poruka obezbeđuju zaštitu od napada koju vrše ubacivanjem starih AAL-SDU ili promenom redosleda u sekvenci AAL-SDU. Zahvaljujući ovome, stare AAL-SDU ili one koje su stigle van redosleda se mogu odbaciti. Ovakva vrsta zaštite se primenjuje na taj način, što se na izvoru prvo dodaje broj sekvence na kraj svake AAL-SDU, a onda računa MAC na ukupnom AAL-SDU, uključujući i broj sekvence. Ovaj MAC, koji štiti i AAL-SDU i broj sekvence, se sada dodaje ukupnom AAL-SDU, koji uključuje broj sekvence. Ova metoda obezbeđuje zaštitu za ATM aplikacije koje nemaju svoj broj sekvence. Kao i za usluge tajnosti, usluga integriteta poruka je specificirana da koristi simetrične algoritme sa tajnim ključem.

Kontrola pristupa. Kontrola pristupa predstavlja primenu pravila koja se zahtevaju za uslugu. Ova pravila zavise od atributa određenog entiteta (identitet), atributa referentnih parametara (ciljna adresa), sistemskih atributa(vreme) i istorije prethodnih zahteva ovog i/ili drugih entiteta korisnika. Kontrola pristupa može se zamisliti kao predikat nad stanjem prostora koji čine svi ovakvi atributi. Ako je predikat zadovoljen, zahtev se prihvata, a ako nije zahtevana usluga se ne izvršava.

Kontrola pristupa u korisničkoj ravni zahteva mehanizam za prenos informacija za kontrolu pristupa, koje se koriste u toku uspostavljanja veze, kao i mehanizam unutar ATM komponenti za korišćenje tih informacija da bi se odredilo da li je pristup vezi odobren. Kontrola pristupa korisničke ravni može biti zasnovana na bezbednosnim labelama (na primer SSL – *Standard Security Label*), identitetima izvornih i odredišnih korisnika, vremenu dana, tipu usluge, poljima viših slojeva ATM protokola (AAL tip) ili drugim parametrima koji se mogu odrediti tokom uspostavljanja veze.

Bezbednosne usluge kontrolne ravni

Kontrolna ravan je mehanizam koji uređajima omogućava da konfigurišu mrežu da bi se postigli određeni ciljevi, na primer, da se uspostave virtuelna komutirana kola. S obzirom na to da poruke kontrolne ravni imaju uticaj na stanje i raspoloživost mreže, njihova zaštita je veoma važna.

U bezbednosnoj specifikaciji mehanizam za signalizaciju je definisan tako da obezbedi strogi kriptografski integritet sa odgovor/preuređenje (*replay/reordering*) zaštitom. Ovaj mehanizam omogućava entitetima kontrolne ravni verifikaciju izvora i sadržaja signalizacionih poruka pre nego što se dodele resursi koji se zahtevaju. Na taj način ATM mreža se štiti od brojnih vrsta napada.

Autentifikacija i integritet. Autentifikacija i integritet kontrolne ravni je ATM bezbednosna usluga, koja povezuje ATM signalizacionu poruku sa njenim izvorom. Kreiranjem ove veze, primalac poruke može na poverljiv način verifikovati da li je poreklo poruke povezano sa navedenim izvorom. Ovo obezbeđuje mehanizam koji eliminiše mnoge pretnje. Tako, na primer, napad odbijanjem usluge, koji se vrši prekidanjem aktivne veze pomoću tajno ubačenih signalizacionih poruka RELEASE (izbacivanje) i DROP PARTY (odbacivanje strana), može se sprečiti proverom autentičnosti signalizacionih poruka u kanalu veze. Ova usluga takođe pruža zaštitu od prevara i zlonamernih izmena. U specifikaciji je definisan mehanizam za autentifikaciju i integritet kontrolne ravni između susednih signalizacionih entiteta. Mehanizam je identičan onom koji je ponuđen za integritet poruka u korisničkoj ravni sa *replay/reordering* zaštitom.

Usluge za podršku

Pomenutom specifikacijom se definiše i skup usluga za podršku koje su potrebne za uvođenje niza bezbednosnih usluga visokih performansi, u koje spadaju:

– bezbednosna razmena poruka i dogovaranje bezbednosnih opcija,

– razmena ključa,

– ažuriranje ključa,
– sertifikacija infrastrukture (engl. *sertfication infrastructure*).

Svaka od ovih bezbednosnih usluga zaslužuje detaljniju analizu.

Bezbednosna razmena poruka i dogovaranje. Da bi se omogućilo funkcionisanje mnogih prethodno opisanih bezbednosnih usluga, potrebno je da uključeni bezbednosni agenti SA (*Security Agent*) prethodno razmene poruke. U specifikaciji su opisane dve vrste razmene bezbednosnih poruka: 1) Razmena poruka unutar UNI 4.0, PNNI 1.0 i AINI (*ATM Inter-Network Interface*) signalizacije, 2) *In-band* razmena poruka, tj. bezbednosna razmena poruka unutar relevantnog virtuelnog kola korisničke ravni, odnosno razmena poruka preko prethodno uspostavljene veze.

Metoda *in-band* razmene poruka, takođe, obezbeđuje i mehanizam za dogovaranje bezbednosnih opcija. S obzirom na to, da se bezbednosni zahtevi menjaju između različitih organizacija, važno je obezbediti raznovrsnost bezbednosnih usluga, algoritama i dužinu ključeva, koji će zadovoljiti široki opseg bezbednosnih potreba. Zbog ovog razloga ATM bezbednosni mehanizam podržava različite bezbednosne usluge, algoritme i dužine ključa. Radi dogovara bezbednosnih agenata oko zajedničkih bezbednosnih parametara, kao što su algoritmi i dužine ključa, metode bezbednosne razmene (koje obezbeđuju dogovaranje pomenutih parametara), uvode se kao deo bezbednosne uspostave VC.

Razmena ključa. Razmena ključa je mehanizam (protokol) pomoću koga dva bezbednosna agenta razmenjuju tajne ključeve, koji se koriste u uslugama tajnosti i/ili integriteta. Ova usluga je često udružena sa uslugom autentifikacije. Ovo se može postići uključivanjem tajnih parametara za razmenu ključa unutar toka poruka za provođenje autentifikacije.

Kao i autentifikacija, razmena ključa se vrši pomoću simetričnih (tajni ključ) ili asimetričnih (javni ključ) algoritama. Razmena ključa može biti bidirekciona (dvosmerna) ili unidirekciona (u jednom smeru).

Ažuriranje ključa sesije. Ključevi sesije su ključevi koji se direktno koriste za obezbeđenje usluga tajnosti i integriteta nad ATM virtuelnim kolom. Zbog potencijalno velike brzine prenosa poruka preko virtuelnog kola, obavezno je da se ključevi periodično menjaju, da bi se sprečilo otkrivanje ključa. Specifikacija 1.1 definiše usluge za ažuriranje ključa. Ova usluga se izvodi u dve faze: faza razmene ključa i faza promene ključa. Faza razmene ključa koristi master ključ (*master key*) koji se razmenjuje prilikom uspostave veze (koristeći usluge razmene ključa), da bi se šifrovao novi ključ sesije. Na prijemu šifrovanog ključa sesije, primalac dešifruje ključ sesije koristeći deljeni master ključ i memoriše ga za drugu fazu, tj. promenu ključa.

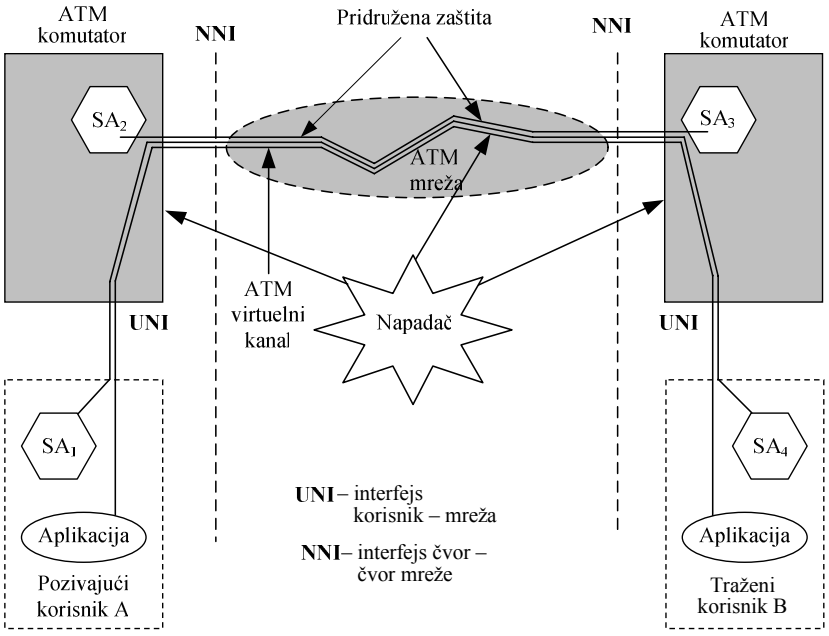
Sertifikacija infrastrukture. U kriptosistemima sa javnim ključem, svaka strana (bezbednosni agent), na primer X ima par ključeva. Jedan od ovih ključeva je javno poznat, to je X-ov javni ključ (PK_x), a drugi je poznat samo X, i to je X-ov privatni ključ (SK_x). Da bi strana X mogla da šalje tajne infor-

macije strani Y (ili alternativno, da bi X bio u stanju da verifikuje digitalni potpis koji je napravio Y), potrebno je da X od strane Y dobije javni ključ PK_y. Iako je PK_y javni ključ, po definiciji ne bi smelo biti omogućeno bilo kojoj strani X da zameni drugu vrednost, na primer, PK_x za PK_y. Da bi se sprečio ovakav tip napada, javni ključ se razmenjuje u obliku „sertifikata".

Sertifikat sadrži ime korisnika, njegov javni ključ i neke dodatne informacije, kao i potpis poverljive ovlašćene osobe – „*Certification Authority*" (CA). Ovaj sertifikat onemogućava krivotvorenje i povezuje javni ključ sa određenom osobom. Bilo koja osoba koja ima pristup CA javnom ključu, može proveriti verodostojnost sertifikata (proverom CA potpisa u sertifikatu) i usvojiti javni ključ koji je sertifikovan. Sertifikat se može prenositi preko nezaštićene veze.

Bezbednosni model ATM mreža

ATM bezbednosni model prikazan je na slici 3, gde su sa SA_i (i = 1, 2, 3, 4) označeni bezbednosni agenti. Bezbednosni agenti iniciraju, uspostavljaju, obezbeđuju, prekidaju i okončavaju bilo koju od bezbednosnih usluga, kao što su kontrola pristupa, autentifikacija, tajnost i integritet poruka.



Slika 3 – ATM bezbednosni model

Pozivajući korisnik A (*initiator*) i traženi korisnik (*responder*) jesu krajnji terminali/sistemi ili krajnje tačke ATM mreže. U ovom bezbednosnom modelu napadač (*intruder*), može da prisluškuje mrežu i komutaci-

one sisteme, registruje sve poruke koje prolaze kroz mrežu i komutacione sisteme, preslušava stare poruke i ubacuje svoje lične informacije u komunikacione nizove slgnala koji se prenose preko ATM mreže.

Da bi komunikacija u ATM mreži bila bezbedna neophodno je da se uvedu sledeće bezbednosne usluge:

– zaštita signalizacije uvođenjem usluge autentifikacije i integriteta,

– dogovaranje bezbednosnih parametara između učesnika u komunikaciji,

– zaštita informacija osiguravanjem tajnosti i integriteta poruka.

Radi dogovara parametara za bezbednosne usluge i direktnu podršku usluge autentifikacije, u ATM bezbednosnoj Specifikaciji 1.0, usvojeni su dvosmerni (engl. *two-way*) i trosmerni (engl. *tree-way*) protokoli za bezbednu razmenu poruka, SME (*Security Message Exchange*).

Dvosmerni SME protokol se može koristiti za uspostavljanje veza tačka-tačka i tačka-više tačaka, u slučaju kada nije potrebno dogovaranje bezbednosnih parametara u okviru UNI 4.0 signalizacije.

Trosmerni SME protokol može se koristiti za uspostavljanje veze i posebno za veze koje zahtevaju dogovaranje bezbednosnih opcija. Implementiran je u *in-band* SME protokolu. U daljem opisu ovih protokola koriste se skraćenice i simboli čije je značenje dato u tabeli 2.

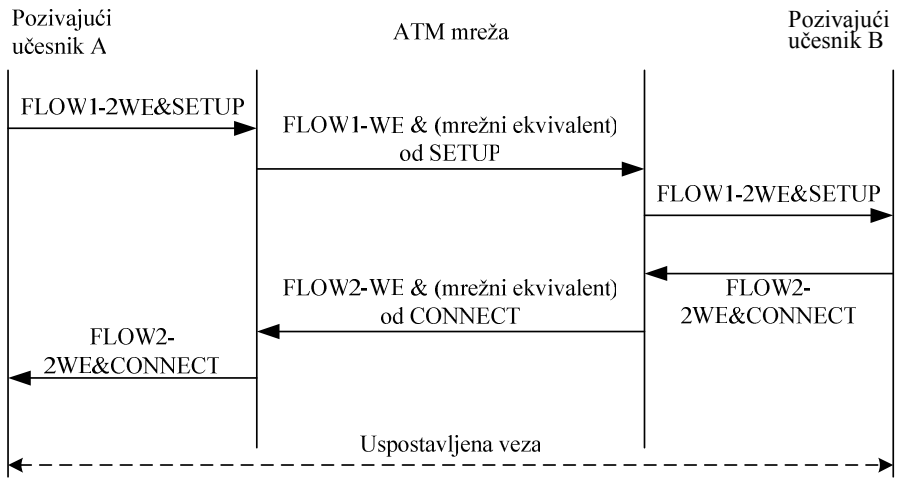
Tabela 2

Značenje simbola i skraćenica

X	Entitet ***X***
K_x	K_x predstavlja javni ključ od ***X*** kada se koristi za šifrovanje, a predstavlja privatni ključ od ***X*** kada se koristi za digitalni potpis
$Enc K_x(text)$	Šifrovan text pomoću ključa od ***X***
$Sig\ K_x[Hash(text)]$	***X***-ov digitalni potpis izračunat nad ***hash*** funkcijom od ***text*** pomoću ***X***-ovog ključa, gde je K_x privatni ključ od ***X***
Hash (text)	Jednosmerna hash funkcija od ***text*** gde je ***hash*** strogo jednosmerna funkcija kao što je ***Secure Hash Algorithm (SHA-1)***
R_x	Slučajni broj koji je ***X*** generisao za ovu priliku
T_x	Vremenski promenljiva markica koju je generisao ***X***
{.}	Oznaka opcije
SecOpt	Ukazuje koje su bezbednosne usluge obezbeđene za vezu
SecNeg	Pozivajući i pozvani entitet koriste $SecNeg_a$ i $SecNeg_b$ da bi dogovorili bezbednosne usluge, opcije i parametre za vezu
ConfPar	Kada se pozivaju usluge za podršku razmene ključa $ConfPar_a$ i $ConfPar_b$ se koriste da sigurno prenesu ključ u vlasništvu jedne strane i to od jedne ka drugoj strani
Cert	$Cert_a$ nosi sertifikat pozivajućeg, a $Cert_b$ pozvanog učesnika

Autentifikacija signalizacionih poruka za uspostavu veze

Autentifikacija signalizacionih poruka za uspostavu veze, u slučaju dvožične veze, obavlja se pomoću dvosmernog SME protokola, na način kako je to prikazano na slici 4.



Slika 4 – Autentifikacija signalizacionih poruka za vezu dva učesnika

Na UNI interfejsu, FOLOW1–2WE SME (dvosmerni SME protokol) prenosi se u SETUP poruci, a FOLOW1–2WE i u CONNECT poruci. Kada korisnik *A* želi da uspostavi vezu sa korisnikom B (prema slici 4) procedura za autentifikaciju zahteva sledeće korake:

Korak 1: Učesnik A šalje *FLOW1–2WE* učesniku *B*

FLOW1–2WE: A → B

Korak 2: Kada *B* primi *FLOW1–2WE* on preduzima sledeće:

- Proverava da li je *B* zaista primalac kome je poruka namenjena.
- Vrši ekstrakciju *SecOp*t i implementira je.
- Verifikuje digitalni potpis i samim time i integritet *FLOW1–2WE.* Digitalni potpis je šifrovan sa tajnim ključem od *A,* koga ima samo *A. B* ga dešifruje javnim ključem od A, pa na taj način dobijenu *hash* funkciju, poredi sa vrednošću *hash* funkcije koju će on izračunati nad primenjenim parametrima. Ako su vrednosti iste, potvrđen je integritet i autentičnost. $ConfPar_a$ je šifrovan sa javnim ključem od *B*, pa ga *B* može dešifrovati svojim tajnim ključem.

- Proverava ekstrakciju R_a za svoj odgovor.
- Vrši ekstrakciju $ConfPar_a$ ako je prisutan i interpretira ga.
- Vrši ekstrakciju $Cert_a$ ako je prisutan i verifikuje njegovu validnost.

Korak 3: Učesnik *B* šalje *FLOW1–2WE* učesniku *A.*
FLOW1–2WE: $B \rightarrow A$

Korak 4: Kada *A* primi *FLOW1–2WE,* on preduzima sledeće korake:

- Proverava da li je A primalac kojem je poruka upućena.
- Verifikuje digitalni potpis, a time i integritet od *FLOW1–2WE.*
- Proverava da li je primljeni R_a u *FLOW1–2WE* identičan onom koji je poslat u *FLOW1–2WE.* Digitalni potpis je šifrovan tajnim ključem od *B*, koga ima samo *B. A* ga dešifruje javnim ključem od *B*, te na taj način dobijenu *hash* funkciju, poredi sa vrednošću *hash* funkcije koju će on izračunati nad primljenim parametrima. Ako su vrednosti iste, potvrđen je integritet i autentičnost. $ConfPar_b$ je šifrovan sa javnim ključem od *A*, te ga *A* može dešifrovati svojim tajnim ključem.
- Vrši ekstrakciju $ConfPar_b$ ako je prisutan i intrepretira ga.
- Vrši ekstrakciju $Cert_b$ ako je prisutan i verifikuje njegovu validnost.

Prema prethodno opisanoj proceduri obavlja se autentifikacija signalizacionih poruka prilikom uspostave veze između dva učesnika.

Dogovaranje bezbednosnih parametara

Bezbednosni parametri se dogovaraju pomoću trosmernog SME protokola, koji se sastoji od sledećih šest koraka:

Korak 1: *A* šalje *FLOW1–3WE* korisniku *B*
FLOW1–3WE: $A \rightarrow B$

Korak 2: Kada učesnik *B* primi *FLOW1–3WE* on preduzima sledeće:

- Proverava da li je *B* zaista primalac kome je poruka namenjena, ako je *B* uključeno u poruku.
- Vrši ekstrakciju $SecNeg_a$ i interpretira ga za svoj odgovor.
- Vrši ekstrakciju poslatog R_a za svoj odgovor.
- Vrši ekstrakciju $Cert_a$ ako je prisutan i verifikuje njegovu validnost.

Korak 3: Učesnik *B* šalje *FLOW2–3WE učesniku A.*
FLOW2–3WE: B → A

Korak 4: Kada učesnik *A* primi *FLOW2–3WE* on preduzima sledeće:

- Proverava da li je *A* zaista primalac kome je poruka namenjena.
- Vrši ekstrakciju $SecNeg_b$ i interpretira ga.
- Verifikuje digitalni potpis i samim tim integritet od *FLOW1–3WE* i *FLOW2–3WE. Hash* funkcija u *FLOW2–3WE* se računa i nad vrednostima koje je učesnik *A* poslao učesniku *B*. Ukoliko dobije ispravnu vrednost za *hash* funkcije, to znači da je učesnik B primio ispravnu poruku *FLOW1–3WE*.
- Proverava da li je primljeni R_a u *FLOW2–3WE* identičan onom koji je on poslao u *FLOW1–3WE.*
- Vrši ekstrakciju poslatog R_b za svoj odgovor.
- Vrši ekstrakciju $ConfPar_b$ ako je prisutan i interpretira ga.
- Vrši ekstrakciju $Cert_b$ ako je prisutan i verifikuje njegovu validnost.

Korak 5: Učesnik A šalje *FLOW3–3WE* učesniku *B.*
FLOW3–3WE A → B

Korak 6: Kada učesnik *B* primi *FLOW3–3WE* on preduzima sledeće:

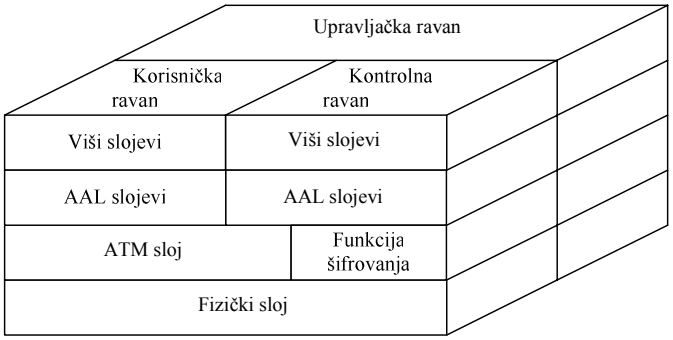
- Proverava da li je učesnik *B* primalac kome je poruka upućena.
- Verifikuje digitalni potpis i time integritet poruke *FLOW3–3WE.*
- Proverava da li je primljeni R_b u *FLOW3–3WE* identičan onom koji je poslat u *FLOW2–3WE.*
- Vrši ekstrakciju $ConfPar_a$ ako je prisutan i interpretira ga.

Prema izloženoj proceduri obavlja se dogovaranje bezbednosnih parametara između dva učesnika pri uspostavi veze.

Tajnost korisničkih poruka

Tajnost korisničkih poruka, koje se prenose preko telekomunikacione mreže, obezbeđuje se šifrovanjem. U ATM mrežama (javne, privatne) šifrovanje se može vršiti na tri načina: na višim slojevima protokola, na ATM sloju, na AAL sloju.

U ATM bezbednosnoj specifikaciji 1.0 šifrovanje je dobilo mesto na ATM sloju, kako je to prikazano na slici 5.



Slika 5 – Položaj funkcija šifrovanje/dešifrovanje u arhitekturi ATM protokola

Pogodnije je da se šifrovanje vrši na ATM sloju zbog fiksne veličine ćelije, jer se na taj način olakšava primena blok-šifri. Kao što je prethodno naglašavano, šifruje se korisnički deo odnosno *payload* ćelije fiksne dužine 48 bajtova.

U prethodno navedenoj ATM bezbednosnoj specifikaciji preporučuju se tri nivoa ključa:

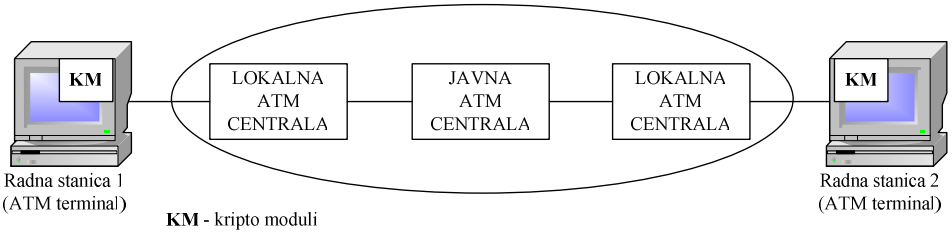
– ključ najvišeg nivoa (engl. *top-level key*) – asimetrični ključ. Ključ najvišeg nivoa se koristi za zaštićenu autentifikaciju i inicijalizaciju prvog ključa sesije i master ključa;

– master ključ (engl. *master key*) – simetrični ključ, koji se koristi za šifrovanje ključa sesije, kada se on ažurira u toku trajanja veze;

– ključ sesije (engl. *session key*) – simetrični ključ, koji se koristi za šifrovanje poruka.

Zaštita komunikacije s kraja na kraj veze u ATM mreži

Širokopojasni ATM terminali, kao što su multimedijalni terminali koji zadovoljavaju IUT-T preporuke H.310 i H.321 (ukoliko se u njih ugrade kriptomoduli za generisanje nekih blok-šifri, digitalnog potpisa i šifrovanje/dešifrovanje), omogućavaju efikasnu zaštitu komunikacije s kraja na kraj veze u ATM mreži (slika 6).



Slika 6 – Blok-šema kriptozaštite s kraja na kraj veze u ATM mreži

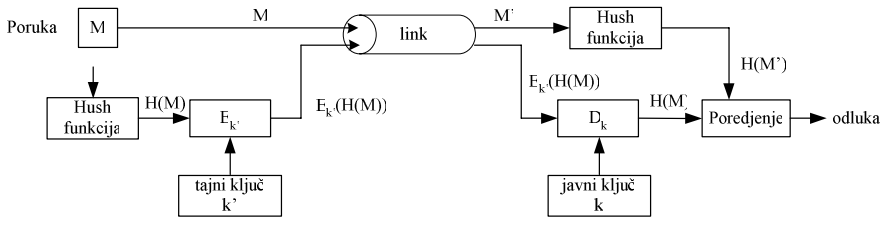
Kao što je poznato, kriptografski algoritmi se dele u dve grupe. U prvu grupu spadaju asimetrični kriptografski algoritmi (sa javnim ključem), a u drugu simetrični kriptografski algoritmi (sa tajnim ključem). Kod simetričnih kriptogafskih algoritama isti tajni ključ koristi se za šifrovanje i dešifrovanje poruke. Ovi algoritmi su mnogo brži od algoritama sa javnim ključem, ali su manje otporni na napade i omogućavaju lakše otkrivanje ključa.

Algoritmi sa javnim ključem koriste dva različita ključa: jedan je javni ključ i koristi se za šifrovanje, a drugi je tajni ključ poznat samo primaocu poruke. Kod ovakvih sistema, čak i kada je poznat metod za šifrovanje E_k i ključ za šifrovanje k (javni ključ) nije lako odrediti algoritam za dešifrovanje $D_{k'}$ i ključ za dešifrovanje k' (tajni ključ). Najpoznatiji takav algoritam je RSA [5]. Ovi kriptografski sistemi su pouzdaniji od simetričnih, ali su mnogo sporiji, pa se koriste u primenama kod kojih bezbednost ima najveći značaj. To su, na primer, razmena simetričnog ključa, koji se koristi za obezbeđenje tajnosti komunikacije između korisnika ili za proces atentifikacije korisnika i proveru integriteta poruka.

Jedna od često korišćenih metoda jeste upotreba *digitalnih potpisa.* Digitalni potpis predstavlja vrstu asimetričnog kripto sistema, a uključuje šifrovanje poruke tako da način šifrovanja zna samo pošiljalac. Ključ za šifrovanje poseduje samo pošiljalac. Digitalni potpis omogućava autentifikaciju učesnika, proveru integriteta poruke i neporicanje. Kao što je prethodno rečeno, autentifikacijom se verifikuje identitet učesnika, proverom integriteta poruke se utvrđuje originalnost poruke tj. da li je sadržaj poruke menjan tokom prenosa preko mreže, a neporicanje onemogućava korisniku da porekne da je poslao neku poruku.

Postoji više načina kreiranja digitalnog potpisa, koji su standardizovani DSS (*Digital Signature Standard*) standardima. Jedan način koristi tzv. *hash* funkciju H (često se naziva i *message digest* – digitalni sažetak poruke). *Hash* funkcija dokument promenljive veličine transformiše u kod fiksne dužine, najčešće kraći od originalne poruke. Time se dokumentu dodeljuje vrednost fiksne dužine.

Princip primene digitalnog potpisa u proceduri autentifikacije prikazan je na slici 7.



Slika 7 – Princip primene digitalnog potpisa u proceduri autentifikacije

Postupak kreiranja digitalnog potpisa je sledeći:

– ako sa *M* označimo poruku, onda *H(M)* predstavlja *hash* vrednost ili digitalni sažetak poruke;

– na ovu vrednost se primenjuje algoritam *E* – šifrovanje privatnim ključem *k'*;

– dobijena vrednost $E_{k'}[H(M)]$ predstavlja digitalni potpis. Ovu vrednost pošiljalac šalje primaocu zajedno sa dokumentom, odnosno originalnom porukom, koja nije šifrovana.

Pri prijemu proces autentifikacije, odnosno provere integriteta poruke (da li je menjana tokom prenosa kroz mrežu), vrši se na sledeći način:

– izračunava se *hash* vrednost primljenog dokumenta (poruke) *H(M')*;

– primenjuje se algoritam dešifrovanja javnim ključem na šifrovanu vrednost digitalnog sažetka $E_{k'}[H(M)]$, koji je primljen zajedno sa dokumentom. Pri tome se koristi algoritam dešifrovanja javnim ključem, koji odgovara algoritmu za šifrovanje privatnim ključem primenjenim na *H(M)*;

– dobijeni rezultat je $D_k\{E_{k'}[H(M)]\}=H(M)$;

– porede se vrednosti *H(M)* i *H(M').* Ako su iste, poruka je originalna i potvrđen je njen integritet. Drugim rečima, to znači da je pošiljalac zaista onaj za koga se pretpostavlja da jeste, jer samo on zna tajni ključ i algoritam dešifrovanja.

Na slici 7 šematski je prikazan prethodno opisani postupak autentifikacije učesnika u vezi. Na ovaj način se ne omogućava pošiljaocu da demantuje da je poslao neku poruku (neporicanje), jer samo on zna tajni ključ *k'* i algoritam $E_{k'}$ koji se ne mogu izvesti iz algoritma dešifrovanja D_k i javnog ključa *k.*

Da bi prethodno opisani postupak bio pouzdan potrebno je da se koriste jednosmerne *hash* funkcije. Takve funkcije imaju dve važne osobine:

– za datu poruku jednostavno je generisati izlazni kod, ali za poznati kod je vrlo teško pronaći poruku čiji je sažetak poznat;

– teško je naći dve različite ulazne poruke, koje za rezultat imaju istu vrednost *hash* funkcije. Primeri ovakvih *hash* funkcija su: SHA-1 (*Secure Hash Algoritam*) i MD5 (*Message Digest 5*).

Drugi sličan način autentifikacije omogućava MAC (*Message Authentication Code*) algoritam. Ovaj algoritam je jednostavniji od algoritma digitalnog potpisa. Osnovna razlika je u tome što se zasniva na simetričnim kripto sistemima, odnosno u tome što koristi dva identična tajna ključa za šifrovanje i dešifrovanje. Omogućava verifikaciju autentičnosti poruke kao i proveru integriteta poruke. Učesnici se pre komunikacije moraju dogovoriti o simetričnim (tajnim) ključevima. Ovaj algoritam ne daje mogućnost neporicanja kao digitalni potpis, zbog toga što koristi simetrične ključeve.

U MAC algoritmu se koristi tzv. *hash funkcija sa ključem* (*keyed hash function*). Ona se dobija tako što se na poruku doda vrednost tajnog ključa, pa se nad celom vrednošću računa *hash* funkcija. Tako dobijena vrednost se naziva MAC kod. Pošiljalac otprema poruku i MAC kod. Primalac računa *hash* funkciju

nad primljenom porukom i tajnim ključem koji je i njemu poznat, a zatim dobijenu vrednost poredi sa dobijenim MAC kodom. Ako su vrednosti iste zaključuje se da je potvrđen integritet poruke i da je verifikovana autentičnost pošiljaoca.

Primeri *hash* funkcija sa ključem su: HMAC-SHA-1 (*Hashing keyed Message Authentication Code*) i HMAC-MD5.

Problemi pri realizaciji bezbednosnih mera i zaštite

Obezbeđenje bezbednosti ATM mreža i zaštita informacija, koje se preko njih prenose, nije ni malo jednostavno. Bez obzira na tehnička rešenja i iskustva koja postoje u rešavanju bezbednosti i zaštite drugih vrsta telekomunikacionih mreža, kod ATM mreža se nailazi na mnoge nove probleme.

Prvi problem predstavlja princip ATM komutacije. ATM komutacioni sistemi – komutatori, mogu se posmatrati kao multiplekseri ćelija velikih brzina [4]. U ATM komutatoru se komutira i multipleksira ćelija tj. serijski niz bajtova fiksne dužine 53 bajta, od kojih pet bajtova čine zaglavlje, a preostalih 48 bajtova (u literaturi se naziva *payload* – korisni sadržaj) prenose informacione sadržaje.

Komutator usmerava – komutira ćelije na osnovu sadržaja zaglavlja u kojem su smeštene adrese virtuelnog kanala i virtuelnog puta na koje se ćelija prosleđuje. Kada je reč o primeni bezbednosnih mehanizama jasno je da se oni moraju primenjivati na ATM ćeliju, odnosno na njen informacioni sadržaj – *payload*. Ako bi smo pokušali da primenimo usluge integriteta i tajnosti i na zaglavlje ćelije, to bi zahtevalo šifrovanje/dešifrovanje u svakom komutatoru. Time bi se mnogo usporila komutacija, pa se takav pristup morao odbaciti. To znači da problem zaštite zaglavlja još uvek nije rešen.

Veliki izazov u procesu zaštite ATM mreža je pronalazak kriptografskog mehanizma koji će zadovoljiti veliku zahtevanu brzinu komutacije u komutatoru. To je veoma važno, jer se kriptografskim tehnikama obezbeđuju važne bezbednosne usluge, kao što su tajnost, autentifikacija i integritet. Većina kriptografskih tehnika radi brzinama mnogo manjim od brzina komutatora koje su reda Gb/s i većim. Postoje hardverske verzije DES koje mogu da rade i na ovim brzinama, ali se javlja novi problem vremena potrebnog za pripremu razmene ključa sesije.

Specifičnost ATM je fiksna dužina ćelije, odnosno fiksna dužina *payload* od 48 bajtova, isključuje mogućnost upotrebe mnogih poznatih kriptografskih mehanizama. Bilo koja blok-šifra sa veličinom bloka većom od 384 bita ne može se primeniti za šifrovanje ATM ćelija. Ako bi se unele niz šifre, javlja se problem resinhronizacije u slučaju gubitka neke ćelije tokom prenosa. Čak i kada se nađe kriptografski mehanizam koji zadovoljava ove zahteve, velika brzina prenosa u ATM mreži uvodi komplikacije u upravljanju ključevima. Na primer, ako ATM radi na 130 Mb/s, to znači da se 0,307M (M-milion) ćelija komutira kroz komutator u jednoj sekundi. Ako koristimo DES šifru sa veličinom

bloka od 64 bita, onda oko 2M blokova DES šifre prolazi kroz komutator u sekundi. Ako broj VC koji rade preko komutatora nije previše veliki, onda sa ovolikom količinom podataka napadač može lako da razbije ključ sesije. Ako pretpostavimo da se jedan ključ ne može koristiti za više od 100 blokova šifri, trajanje jednog ključa sesije postaje kratko i iznosi nekoliko stotina sekundi. To mnoge tradicionalne blok-šeme za razmenu ključeva čini neadekvatnim. Ako bismo našli šemu koja bi menjala ključ sesije ovom brzinom, javlja se problem permanentnog (master) ključa, koji se koristi za šifrovanje ključa sesije. Česta promena ključa sesije može dovesti do otkrivanja permanentnog ključa.

Prema pomenutim preporukama ATM Foruma, zaštita se primenjuje i na virtuelnim kolima (VC). To znači da se za svako VC primenjuje različit ključ. Jedna od prednosti ovakvog pristupa je što je zaštićena tajnost drugih VC i ako je jedno VC ugroženo. Druga prednost je relativno dug „životni vek“ ključa sesije, pod pretpostavkom da saobraćaj nije tako veliki kao saobraćaj celog sistema. Ovom metodom sistem može obezbediti kvalitet bezbednosnih usluga za različita VC, čime se uvodi koncept kvaliteta usluga QoS u ATM bezbednost. I u ovom pristupu postoje neke otežavajuće okolnosti. Šifrator mora veoma brzo pristupiti širokom opsegu ključeva. Takođe, zahteva se da šifrator veoma dinamično menja ključ sesije, kao i da veoma brzo može pristupiti sledećoj ATM ćeliji. Ovaj zahtev, koji se naziva agilnost ključa, nije ni malo jednostavan. Ako se uzme u obzir i potencijalno veliki broj VC, traženje ključa u velikoj tabeli ključeva unosi dodatno kašnjenje.

Zaključak

Međunarodna unija za telekomunikacije – ITU (*International Telecommunications Union*) prihvatila je asinhroni način transfera kao tehniku prenosa, multipleksiranja i komutacije kao buduću svetsku digitalnu širokopojasnu mrežu velikih bitskih protoka. Ta mreža omogućava prenos svih vrsta medija, odnosno informacija (govor, video, podaci, mirne slika, multimedijalne poruke) na jedinstvenoj tehnološkoj osnovi. ATM mreže koriste se u javnim telekomunikacijama, kao i u privatnom okruženju, a njihovi korisnici su i namenski sistemi (vojska, policija).

Može se reći da će buduće ATM mreže prenositi internet saobraćaj, javni telefonski saobraćaj, komercijalne komunikacione aktivnosti, kao i vojne aplikacije. Za sav telekomunikacioni saobraćaj, bez obzira na to o kojem korisniku se radi, bezbednost ovih mreža nameće se kao ključni problem.

Bezbednost ATM mreža pojavila se kao problem kada se uvidelo da su ugrožene raznim vrstama pretnji i napada. Od 1995. godine do danas traje rad radne grupe ATM Foruma za pitanja bezbednosti, kao i drugih grupa na uvođenju bezbednosnih usluga u ATM, radi obezbeđenja sigurne komunikacije. Ovaj rad nije usmeren na iznalaženje i definisanje novih bezbednosnih mehanizama, nego na korišćenje postojećih bezbednosnih tehnika, kao što su razne vrste algoritama za šifrovanje/dešifrovanje, digitalni potpis i druge postojeće tehnike.

Do sada su donete dve bezbednosne specifikacije (preporuke) – Verzija 1.0 i Verzija 1.1, kao i brojni dodaci, ali time ipak nisu rešena sva pitanja ATM bezbednosti. Ostalo je nerešeno pitanje bezbednosti kontrolne ravni, bezbednosti upravljačke ravni, kao i još neki zahtevi. Rad na uvođenju ovih bezbednosnih usluga dosta je otežan zbog raznih poteškoća i protivrečnih zahteva pomenutih u prethodnom odeljku.

Osnovni pristup i koncept bezbednosti u ATM, kako je sugerisano u pomenutim bezbednosnim specifikacijama ATM Foruma, sastoji se u obezbeđenju bezbednosti na nivou virtuelnog kola (VC). To je od velike važnosti, jer se time omogućava uvođenje kvaliteta usluga – QoS i u područje bezbednosti ATM. Treba imati u vidu da je kvalitet usluga QoS (engl. *Quality of Service*) jedna od najznačajnijih karakteristika ATM mreža.

Na problemima bezbednosti ATM mreža ne rade samo radne grupe i članovi ATM Foruma. U literaturi [3], [7], [8] mogu se naći brojni predlozi za poboljšanje specifičnih bezbednosnih usluga. Autori su uglavnom obradili: slabosti komunikacionih ATM protokola, razne načine obezbeđenja autentifikacije i tajnosti, kontrolu pristupa realizovanog korišćenjem jedne vrste vatrenog zida (ATM *Firewall*), itd.

U ovom radu prikazan je pregled problema i rešenja bezbednosti ATM mreža. Navedene su neke od mogućih pretnji i napada kojima su ATM mreže izložene, definisani su ATM bezbednosni ciljevi, kao i funkcionalni zahtevi mrežnog ATM sistema. Takođe, prikazan je način primene ovih ciljeva na ATM arhitekturu protokola, te ukratko opisane ATM bezbednosne usluge. Objašnjen je model ATM bezbednosti, a prikazane su takođe *two-way* i *three-way* MSE procedure za autentifikaciju i dogovaranje bezbednosnih parametara. Navedeni su neki od problema, koji se javljaju pri uvođenju tehničkih rešenja bezbednosti ATM mreža.

Sa sigurnošću se može reći da je potrebno još mnogo vremena i napora da se konačno i uspešno reše sva pitanja bezbednosti ATM mreža. Treba imati u vidu da napadači na mrežu postaju sve spretniji, ali nastaju i sve savremeniji bezbednosni algoritmi. Nema sumnje da se borba između napadača i korisnika nikada neće završiti, ali je cilj da se bude bar dva koraka ispred napadača.

Literatura

[1] ATM Security Framework 1.0, ATM Forum Technical Committee, february 1998.

[2] ATM Security Specification 1.0, ATM Forum Technical Committee, february 1999.

[3] ATM Network Security: – Vulnerabilities and Risks – white paper.

[4] Jevtović, M., *Telekomunikacione ATM mreže*, Grafo-Žig, Beograd, 2001.

[5] Jevtović, M., *Multimedijalne telekomunikacije*, Grafo-Žig, Beograd, 2004.

[6] ATM Security Specification version 1.1, ATM Forum Technical Committee, march 2001.

[7] ATM Network Security**,** www.atm forum. com

[8] Securing Communications over ATM Networks, white paper.

SECURITY AND PROTECTION IN THE BROADBAND ATM TELECOMMUNICATION NETWORKS

Summary:

Security of communications over broadband ATM networks is analysed in this paper. Attacks on ATM networks (faber tapping, SONET (Synchronous Optical network) drop/add multiplexor attacs, eavesdropping, spoofing, virtual channel stealing, service denial, traffic analysis, protocol weaknesses, ILMI (Integrated Local Management Interface) attacs, PNNI (Private Network to Network Interface) attacks), model of ATM and ATM security framework are described. Some problems occurring within security and protection realization in the communication over ATM networks are also specified.

Key words: *Telecommunication networks, Asynchronous Transfer Mode – ATM, broadband networks, network security, protection of networks and information, model of ATM nerwork security.*

Datum prijema članka: 31. 12. 2008.

Datum dostavljanja ispravki rukopisa: 16. 03. 2009.

Datum konačnog prihvatanja članka za objavljivanje: 30. 03. 2009.